STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G7: Video Tele-Conferencing (VTC) Security

1. INTRODUCTION:

Video Tele-Conferencing (VTC), or video conferencing, is an extension of traditional telephony technologies, which provides aural communications with the additional features of visual communications and information sharing.

While traditional telephone systems have few vulnerabilities and present minimal or no security risk, this is not the case for Internet Protocol (IP) based or network connected VTC endpoints. These VTC endpoints are riddled with security deficiencies and issues due to their many useful features, connectivity options, and minimal built-in support for security controls.

There exists a natural conflict between making VTC systems work and making them secure. Voice communications and video communications on an IP network use essentially the same protocols, have the same IP vulnerabilities, and have the same security issues with firewalls.

2. OBJECTIVE:

Provide guidance for securing IP-based VTC systems and communications.

3. SCOPE:

These guidelines are recommended for all State of Alabama organizations that plan, manage, or utilize VTC technology.

4. GUIDELINES:

The following guidelines, based on the recommendations of the National Security Agency (NSA) and other best practices, should be used to secure the VTC systems, communications, and collateral information.

- Use the latest stable version of firmware and software; apply patches as required.
- Configure unique hard to guess remote access password and change passwords at least every 90 days. Do not use default accounts.
- Ensure passwords meet or exceed the requirements of State IT Standard 620-03S1.
- Ensure passwords are not displayed in the clear during logon.
- Configure unique hard to guess room password (physical access), and rotate periodically.
- Configure unique hard to guess SNMP community string, and rotate periodically. Ensure the default SNMP community strings (e.g., “public” and “private”) are changed prior to placing the system into service. Ensure SNMP community strings are managed like passwords.

- Disable remote monitoring and web snapshots.
- Disable far-end camera control.
- Disable streaming capabilities.
- Disable all wireless functionality.
- Disable unnecessary features (FTP, HTTP, TELNET).
- Enable encryption for all calls (Set to auto at a minimum).
- Encrypt traffic between VTC units and management station.
- Disable auto-answer for incoming calls.
- Use 'Do Not Disturb' after all parties have connected and when no calls are expected.
- Ensure ringer volume is at an audible level.
- Use a security banner/welcome screen to advise users that they are accessing a Government information system and provide them with the appropriate privacy and security notices.
- Take a snapshot of all system files and periodically verify that they have not been modified.
- Use access control lists and firewall rules to secure VTC networks.
- VTC systems should be logically separated on the Local Area Network (LAN) from themselves and other LAN services. Separate VTC systems from the rest of the IP network using Virtual LANs.
- Physically secure VTC devices.
- Limit access to management server via strict access control lists.
- Utilize inactive session timeout feature to disconnect idle/inactive management connections or sessions. Set timer to a maximum of 15 minutes.
- Use HTTPS, SSH, or other secure service for device management.
- Turn off VTC device and cover camera lens when not in use.
- Conduct routine security audits of VTC devices.
- Do not publish network diagrams or VTC phonebooks.

5. DEFINITIONS:

COLLATERAL INFORMATION: Information that is in the workspace that is not meeting or conference related but can be seen by the camera or heard by the microphone. Collateral information can also be non meeting/conference related information on a PC workstation that is used to participate in, or present to, a conference.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 620-03S1: Authentication - Passwords

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	9/12/2008	